SANDIA REPORT
SAND2020-3908
Printed April 2020

Sandia National Laboratories

The Always/Never Safety Framework for Satellite Rendezvous and Proximity Operations and On-Orbit Servicing

Celeste A. Drewien, Roger C. Byrd, Scott E. Slezak, and Mark R. Ackermann

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

Space rendezvous and proximity operations are increasing in numbers, enabling inspections, diagnostics, and maintenance of on-orbit systems. Because collision, loss of control, and unintended damage can impact the system under examination—and at the extreme, cause system break-up and space debris—the safety practices for rendezvous and proximity operations can have significant implications for national security.

This study examines the applicability of the Always/Never surety framework, which was developed for United States nuclear weapons, as a model safety basis for unmanned space proximity operations. This unclassified framework has understandable safety approaches and principles and focuses on a system being always safe—never unsafe. The authors consider that the adapting the framework might present a means for standardization across government and commerce, encouraging a consistent approach and a set of clarifying safety principles and applications for rendezvous and proximity operations. The framework also offers a consistent taxonomy, presents safety and reliability requirements organized by four environment categories, defines accident or abnormal conditions, contributes a strategy for identifying hostile and tactical environments, and enables decision-making for determining if conditions are safe for proximity space operations.

ACKNOWLEDGEMENTS

The authors acknowledge Drew Woodbury for championing this study, the Systems Analysis Group management team for funding and managing this effort, and Jeff Apolis, Nancy Hayden and Munaf Aamir for their peer reviews of this work. The authors and sponsors also thank J J Hogan for hosting the presentation of this work at the Pentagon and enabling connections within the Department of Defense and the Consortium for Execution of Rendezvous and Servicing Operations.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
AIAA	American Institute of Aeronautics and Astronautics
ASARP	as safe as reasonably practicable
COLA	collision avoidance
CONFERS	Consortium for Execution of Rendezvous and Servicing Operations
EMP	electromagnetic pulse
EMR	electromagnetic radiation
ESA	European Space Agency
ESD	electrostatic discharge
IAEA	International Atomic Energy Agency
ISO	International Standards Organization
km	kilometer
lbs	pounds
LEO	low Earth orbit
m	meter
NASA	National Aeronautics and Space Administration
NPS	nuclear power source
NW	nuclear weapon
OOS	on-orbit servicing
RISC	risk-informed safety case
RPO	rendezvous and proximity operation
SCA	safety collision avoidance
sec	second
SOH	state of health
SSA	space situational awareness
TNT	trinitrotoluene
UNCOPUOS	United Nations Committee on the Peaceful Uses of Outer Space
US	United States
UU	unknown and underappreciated hazard

This page left blank

1. INTRODUCTION

In the late 1950s Sandia National Laboratories (Sandia) began working in space technology, including satellite systems and sensors, and the labs have continued such work to the present day. The labs' focus on national security and strategic futures drives a motivation to understand the interaction between technology and policy in the space domain. The work of Sandia National Labs has significantly contributed to nuclear weapon surety policy and technology. The term "surety" comes from Sandia's work in the engineering of the US nuclear deterrent, and it represents the requirements for safety, security, reliability, and use control — which underly policy and can affect or influence technologies or practices. There are lessons from the doctrine of nuclear weapon (NW) surety that can be applied to the safety, security, reliability of space assets and may contribute to the advancement of space policy and technology.

Space rendezvous and proximity operations (RPO) have the potential to influence Sandia's space technology. These operations enable inspections and diagnostics of on-orbit systems by bringing satellites close (<10 km) to one another through a series of orbital maneuvers. On-orbit servicing (OOS) operations place and maintain a spacecraft in the vicinity of (that is, <1 km distance and <0.1 m/sec velocity) or attached to an object for purposes of:

- Inspection
- Capturing or deploying
- Docking and undocking
- Repairing
- Performing maintenance
- Refueling
- Removing from orbit
- Other activities

As unmanned space rendezvous and proximity operations become more common, the associated safety practices become a concern. Collision, electrical failures, programming faults, miscommunication, loss of control, and unintended breakup due to explosion or mechanical failure—all can impact the system under examination. At the extreme, they can cause system break-up and space debris that interfere with launch timing and create collision obstacles that must be tracked to ensure the safety of other spacecraft on orbit.

The space environment is also naturally hazardous "and is increasingly congested, contested, and competitive".[1] The uncertainty of the space environment adds to the RPO/OOS safety concerns. The high consequences of unsafe operations—such as mission failure due to loss of one or both satellites and/or space debris that interferes with, degrades, or destroys other spacecraft—can often have national security implications.

[1] Joint Publication 3-14, "Space Operations", (10 April 2018); https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwicgtH3o8jnAhUTvZ4KHZwxCC4QFjAAegQIARAB&url=https%3A%2F%2Fwww.jcs.mil%2FPortals%2F36%2FDocuments%2FDoctrine%2Fpubs%2Fjp3_14.pdf&usg=AOvVaw0aHb_eA_YDi0zMekWsix7K

Safe proximity operations can prevent accidents and their ensuing hazards. Guidelines for safety of unmanned satellite RPO and OOS are emerging.[2] A technical framework that would benefit safety for government and commercial RPO/OOS is needed.

1.1. Space Safety Standards and Frameworks

A survey of existing space safety frameworks and standards reveals few open-source documents that cover technical safety frameworks for on-orbit unmanned space vehicles. The relevant literature includes the following examples.

1.1.1. MIL-STD-882E

This Military Standard (MIL-STD-882[3]) for satellite system safety was initially released in 1969 and has been updated through several versions. "MIL-STD-882 identifies the Department of Defense's systems engineering approach to eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated. It covers hazards as they apply to systems, products, equipment, and infrastructure (including both hardware and software) throughout design, development, test, production, use, and disposal."[4] The definition of hazard is "any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property, or damage to the environment". For military space systems, this standard still applies.

1.1.2. United Nation's Safety Framework for NPS Applications in Outer Space

A joint document of the International Atomic Energy Agency (IAEA) and United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) Scientific and Technical Subcommittee provides a safety framework for nuclear power source (NPS) applications in outer space. Technical and programmatic elements are included in the framework, whose purpose is to guide nations in developing safety practices that will mitigate risks arising from the use of NPS applications in their space systems.[5] While the focus of this study does not include NPS, safety due to the presence of an NPS on a satellite undergoing RPO/OOS could be encompassed by the technical framework presented herein.

1.1.3. NASA System Safety Framework

The National Aeronautics and Space Administration (NASA) System Safety Handbook[6] presents a procedural framework to guide system safety activities towards satisfaction of defined safety objectives and organize safety products and activities. The steps of this system safety framework

---

[2] "CONFERS Recommended Design and Operational Practices" (1 Feb 2019) and "Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS)", (7 Nov 2018); https://www.satelliteconfers.org/publications/

[3] Department of Defense, "Standard Practice for System Safety", MIL-STD-882E (May 11, 2012)

[4] NASA System Safety Handbook, vol. 2, version 1.0, NASA?SP-2014-612 (November 2014) p. 5; ntrs.nasa.gov › archive › nasa › casi.ntrs.nasa.gov

[5] "Safety Framework for Nuclear Power Source Applications in Outer Space", Document jointly prepared by the UNCOPUOS Scientific and Technical Subcommittee and the International Atomic Energy Agency (2009), UNA/AC.105/934; https://www.esa.int/About_Us/ECSL_European_Centre_for_Space_Law/Nuclear_Power_Sources_NPSs#Document

[6] NASA vol. 1, p. 8; https://ntrs.nasa.gov/search.jsp?R=20120003291

consist of safety objective identification, safety requirements setting, safety ensurance (translating safety objectives into safety requirements), safety assurance, and risk acceptance. The process addresses unknown and underappreciated hazards (UUs) and sets decisions using a risk-informed safety case (RISC) as one of the evaluation bases. The framework is intended for use by commercial service providers to support risk-informed development of safety performance requirements for cargo and crew transportation to low Earth orbit (LEO). It allows flexibility in how requirements are met and substantiated. Continuous improvement—from a minimum tolerable level of safety to a desirable level—enhances system studies and development while imposing NASA's "safety-first" core value policy.[7] The present study does not present the procedures underlying the Always/Never framework, yet the authors note that the steps of the NASA framework bear strong similarity to the NW safety framework.

1.1.4. CONFERS Safety Framework

The Consortium for Execution of Rendezvous and Servicing Operations (CONFERS) [8]—an industry-led initiative focused on non-binding, consensus-derived technical and operations standards for RPO and OOS—has drafted a safety framework for satellite servicing. This Technical and Operational Guidance Document[9] introduces a common lexicon and structure (or ontology) for satellite servicing stakeholders. It provides best practices, guidelines, and standards for safety in the various phases of a satellite servicing mission. The twelve RPO/OOS stages, shown in Figure 1-1, describe how a "client" satellite in its orbit is assisted by a "servicer". A client may be cooperative if it contains on-board navigational aids for rendezvous and docking, or non-cooperative if it does not. CONFERS explains design and mission assurance considerations for safety, including guidance, navigation, and control system needs; sensor suites and calibration for cooperative and non-cooperative client operations; and fault detection.

The framework puts forth safety considerations for docking, grappling, and propellant transfer, and it advises on electrostatic discharge (ESD) mitigation and electromagnetic interference and compatibility. The safety risks across the stages of an RPO/OOS are mapped and explained in this draft framework.

[7] NASA vol. 2, p. 6
[8] https://www.satelliteconfers.org/about-us/
[9] CONFERS Satellite Servicing Safety Framework Technical and Operational Guidance Document Draft (April 2018)

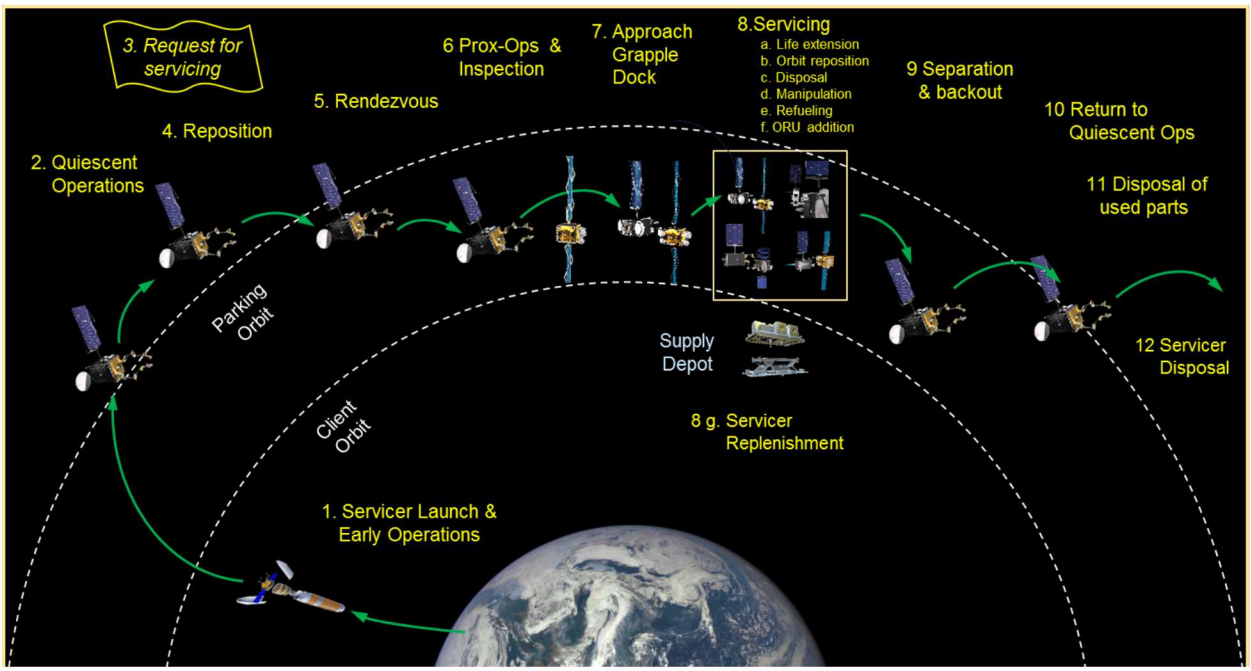

Figure 1-1. Satellite Servicing Mission Operations (CONFERS)

2. SANDIA AND THE ALWAYS/NEVER SURETY FRAMEWORK

Through seven decades of nuclear weapons work, Sandia and others in the US nuclear weapons enterprise developed the Always/Never surety framework with technical and programmatic elements around safety, security, and control[10] of nuclear weapons. The Always/Never standard for nuclear weapons means that they must always be available, reliable, and safe for use when needed and never be unsafe or go off unless authorized[11]. Nuclear weapons are subject to the most precise and stringent command and control, safety, and security possible to prevent accidental or inadvertent nuclear explosions[12]. While accidents with US nuclear weapons have occurred, no accidental nuclear detonation has ever resulted.

The NW system safety portion of the Always/Never surety framework implements "positive measures to minimize the possibility of detonation from accidents, unauthorized actions, inadvertent errors, or acts of nature".[13] "Nuclear safety also encompasses design features and actions to reduce the potential for dispersal of radioactive materials in the event of an accident."[14]

The foundational elements of the NW safety design framework are discussed in the following sections.

2.1. NW Safety Definition

The first element of the safety framework is defining the safety objectives. Sandia defines weapon safety as the organized activities concerned with the prevention of unintended nuclear detonations and the scatter of radioactive materials from nuclear weapons.

The Department of Defense defines nuclear weapon system safety as, "The application of engineering and management principles, criteria, and techniques to protect nuclear weapons against the risks and threats inherent in their environments within the constraints of operational effectiveness, time, and cost throughout all phases of their life cycle."[15]

The safety definition is easily encapsulated by the "Always/Never" expression, enabling ease of retention and understanding—always safe/never go off unless authorized.

2.2. NW Safety Requirements

Requirements are derived from safety objectives. NW requirements have evolved and standardized for several decades. The critical safety requirements are that there be no accidental explosion yielding greater than four pounds trinitrotoluene (TNT) equivalent and no dispersal of special nuclear materials. Other requirements exist, such as the probability of remaining safe in specific environments.

---

[10] DoD surety definition from (DoDD 3150.02 (April 24, 2013): "Policies, procedures, controls, and actions that encompass safety, security, and control measures, which ensure there will be no nuclear weapon accidents, incidents, unauthorized detonation, or degradation of weapon effectiveness during its STS."

[11] See for example https://www.kirtland.af.mil/News/Article-Display/Article/817375/sandia-labs-documentary-gives-detailed-history-of-nuclear-weapons/

[12] Alton P. Donnell, Jr., "A Robust Approach to Nuclear Weapon Safety", SAND2011-4123C, Sandia National Laboratories, Albuquerque, NM (2001)

[13] OSD, Nuclear Weapons Handbook, https://www.acq.osd.mil/ncbdp/nm/NMHB/chapters/chapter_7.htm

[14] Ibid.

[15] DoDM 3150.02, "DoD Nuclear Weapon System Safety Program Manual", (January 31, 2016)

2.3. NW Safety Principles

The NW safety design basis relies on the use of safety principles in design and implementation. For ease of retention and recollection, the principles ensuring safety are encapsulated by the "3I's":

- **Isolation**—the predictable separation of weapon elements from compatible energy
- **Incompatibility**—the use of energy or information that will not be duplicated inadvertently
- **Inoperability**—the predictable inability of weapon elements to function

In addition, there is also the little "i" for the principle of **independence** of safety subsystems and components with differing properties and functions to prevent common cause/mode failures—some refer to independence as the "4th I".

Elimination of safety hazards by design selection, operation, and logistics is also implemented.

The "3I's", "independence", and "elimination" provide an easy means to remember, communicate, and implement safety principles.

2.4. NW Stages of the System Lifecycle

As with the CONFERS safety framework, the stages in a NW lifecycle are defined in the Always/Never framework in order to consider potential energy sources present in operational environment or logistics that might serve as safety hazards. Generic lifecycle stages include transport, handling, storage, maintenance, and deployment. Substages are defined within the main stages as needed.

2.5. NW Environments

Environments are identified by the following categories and then assessed for hazards—electrical, mechanical, thermal, chemical, etc.—in each stage of the lifecycle.

- In a **normal environment**—natural or man-made situations that are expected to occur during the day-to-day logistics and operation of the weapon over its lifetime—the NW must always remain reliable and safe.
- In an **abnormal environment**—accident or unexpected events—the NW is not expected to retain operational reliability, but it must remain safe—never detonate. Abnormal environments are identified by considering logistics and operational scenarios including the inherent risks and threats.
- In a **hostile environment**—defined as the environment created by the nearby detonation of an enemy's nuclear weapon—a NW has reliability requirements and may have logistics-dependent safety requirements.
- **Tactical environments** refer to any unintended but unavoidable environment generated by an emergency tactic or maneuver necessary to maintain safety, security, and control of nuclear weapons.

Once established as normal, abnormal, or hostile, the Always/Never condition applies through the reliability and safety requirements summarized in Table 2-1.

Table 2-1. NW Environments and Safety Requirements

Design-Basis Environment	Definition	Reliability Requirement	Safety Requirement
Normal	Planned and expected	Remain reliable	Remain safe
Abnormal	Accident of beyond design basis for mission reliability	Treat as unreliable	Remain safe
Hostile	Deliberate threats	No severe degradation in reliability for design basis	Remain safe, per mission-specific needs

2.6. Use of NW Safety Framework

From the start of the Cold War, the NW safety design basis was kept unclassified in order for the US to share safety technologies and many procedures with other nuclear weapon nations. The intent was that if other nations had nuclear weapons, the US wanted those weapons to be as safe as practicable. It was believed that simply sharing of the safety framework, including safety system architectures and component designs, might reduce the probability of an unintended nuclear detonation.

From the start of the Cold War, the NW safety design basis has been kept unclassified in order to promote the sharing of US safety technologies and procedures.

Being unclassified, the safety framework is available for use in other arenas—such as the space domain. While satellites may not need the rigor and stringent command, control, and safety of nuclear weapons, the uncertainty of RPO and the space environment—along with consequences for mission failure and debris generation—make it interesting to consider whether the Always/Never safety framework or elements of it add value to the RPO/OOS community.

This page left blank

3. PURPOSE AND APPROACH

3.1. Purpose

In this study, the authors consider the adaptation of the NW Always/Never surety framework to satellite RPO/OOS. This study investigates the steps necessary to apply the Always/Never safety design framework to unmanned RPO/OOS and demonstrate what learning, if any, can be gained by applying the Always/Never safety framework to RPO/OOS.

3.2. Methodology

To this end, the authors follow the NW Always/Never framework, using it to:

- Define RPO/OOS safety objectives
- Identify RPO/OOS stages of operation
- Define RPO/OOS environments and associated requirements
- Recognize RPO/OOS scenarios

This study involved a conceptual analysis to determine the general utility of the framework to RPO/OOS. While the focus was on safety, reliability requirements are also mentioned.

Possible effects due to different orbits are not examined. Orbit types and altitudes will affect specifics of environments, but the basic framework can be generically applied. Specific utility of the framework would require details of RPO/OOS operations and requirements, which can be product-dependent and possibly unique. These details would therefore be examined by procuring agencies, who could use the Always/Never framework during needs analysis and early product development.

This page left blank

4. DEFINING THE RPO/OOS TECHNICAL SAFETY FRAMEWORK

4.1. RPO/OOS Safety Definition

The first item in the framework is a definition of safety. In surveying the literature, a variety of guidance and definitions arise for spacecraft, satellites, and RPO/OOS safety:

- CONFERS provides guidance for RPO safety—**minimize likelihood of and adverse consequences from collisions and generating space debris.**[6]
- NASA[16] and Mil-Std-882E define safety as **freedom from those conditions that can cause** death, injury, occupational illness, **damage to or loss of equipment or property, or damage to the environment.**
- NASA Safety Standard Volume 1 adds **freedom from conditions that cause loss of mission.**
- RPO/OOS safety focuses on distance and velocity as important factors for the final approach maneuver prior to braking.[5]

Due to variations in mission and needs, no one definition exists across the various entities defining safety—however, broad objectives are articulated.

4.2. RPO/OOS Safety Requirement

The satellite community, if not governed by NASA's Procedural Requirements, broadly abides by the principle of "do no harm", which may be ambiguous but is usually understood to mean minimize debris and do not impact the mission of the host platform. This consideration includes avoiding collisions. For RPO/OOS, "do no harm" implies the client does not harm the servicer, and the servicer does not harm the client.

Other safety requirements can be derived from the mission objectives and safety definitions. Some of the implied requirements found in the literature include:

- Use of a collision avoidance (COLA) course and a safety ellipse
- Minimize contamination
- Minimize radio-frequency interference
- Control and minimize damage from electrostatic charging
- Minimize blocking/shadowing of client components
- Comply with orbit debris requirements

Recommendations include:

- Use autonomous fault detection and response mechanisms
- Provide a "safe" configuration to prevent damage to RPO/OOS
- Have a plan for communicating with the client's operations center

[16] See for example, NPR 7120.8A, NPR 8715.3, NPR 8715.7A; NASA Procedural Requirements, "NASA Research and Technology Program and Project Management Requirements", NPR 7120.8 (September 14, 2018); https://nodis3.gsfc.nasa.gov/displayAll.cfm?Internal_ID=N_PR_7120_008A_&page_name=all

4.3. RPO/OOS Safety Principles

NASA[17] addresses safety principles—an adequately safe system is one that adheres to the following fundamental safety principles:

1. Meeting minimum tolerable levels of safety, and
2. Being as safe as reasonably practicable (ASARP).

Safety design principles organized like the 3I's are not readily available.

4.4. RPO/OOS Stages of the Lifecycle

Table 4-1 identifies generic stages of RPO/OOS based on differing responsibilities, environments, and requirements. Sub-stages may be distinguished to further categorize normal operational procedures and specific environments encountered within a stage. For example, soft docking environments could differ from mating environments, due to mechanical forces. The table also contains an attempt to map generic stages to the CONFERS stages identified in Figure 1-1. Note that Launch and Quiescent Operations are not included in the RPO/OOS stages presented here because the focus is only on the stages specific to on-orbit operations and because launch safety—particularly manned spacecraft—is well established[18].

Table 4-1. RPO and OOS Stages of Operation

Stage	CONFERS Stages	Definition
Transit	Reposition	Flight outside the approach ellipsoid surrounding a space object; may include phasing
Approach	Rendezvous, Prox-Ops & Inspection, Approach	Movement within the approach ellipsoid (e.g., 4x2x2 km) and keep-out sphere; final approach is within meters to contact
Docking	Grapple, Dock	Physical contact, including soft docking with and extendible interface and hard docking in which full physical connection is achieved, and de-spin
Service/Capture[19]	Servicing	Integrated operations
Undocking	Separation	Release of physical connections and separation
Depart	Backout	Movement away, exiting the approach ellipsoid

Here the stages are defined using the notion of a boundary approach ellipsoid, a keep-out sphere, and a keep-out zone for safety. A keep-out region may be defined for rendezvous. The keep-out sphere and zone may trigger the start and stop of substages for docking operations, including safe distances for abort or other operations prior to docking. A notional approach ellipsoid is illustrated in Figure 4-1.

[17] NASA Space System Safety Handbook volume 1, p. 15
[1818] See for example NASA Standard 8719.25; https://ntrs.nasa.gov/search.jsp?R=20180001258
[19] Note that Capture implies non-cooperative interaction.

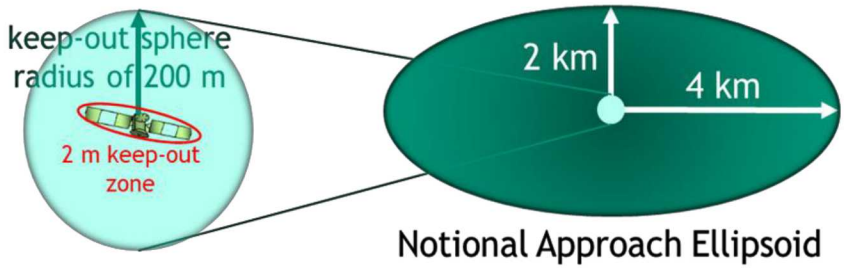

Figure 4-1. Notional Approach Ellipsoid for RPO

4.5. RPO/OOS Environments

Space environments are defined—some very specifically and others generically—subject to the exact conditions to the mission need. NASA refers to environments as natural or induced[20]. The American Institute of Aeronautics and Astronautics (AIAA) has conferences and publications on atmospheric and space environments. The International Standards Organization (ISO) and European Space Agency (ESA) have standards for space environments—much of the focus is on natural radiation environments. A more comprehensive view of environments is provided by the Always/Never framework, which defines categories that differentiate the safety and reliability requirements within the environment types. Using the Always/Never framework, Figure 4-2 shows environments that may be encountered during an RPO or OOS. Environments are categorized by their expected conditions: (normal), unexpected (abnormal), threat (hostile attack), and counterthreat (tactical measures). The literature and standards on space environments do not contain tactical and abnormal environments.

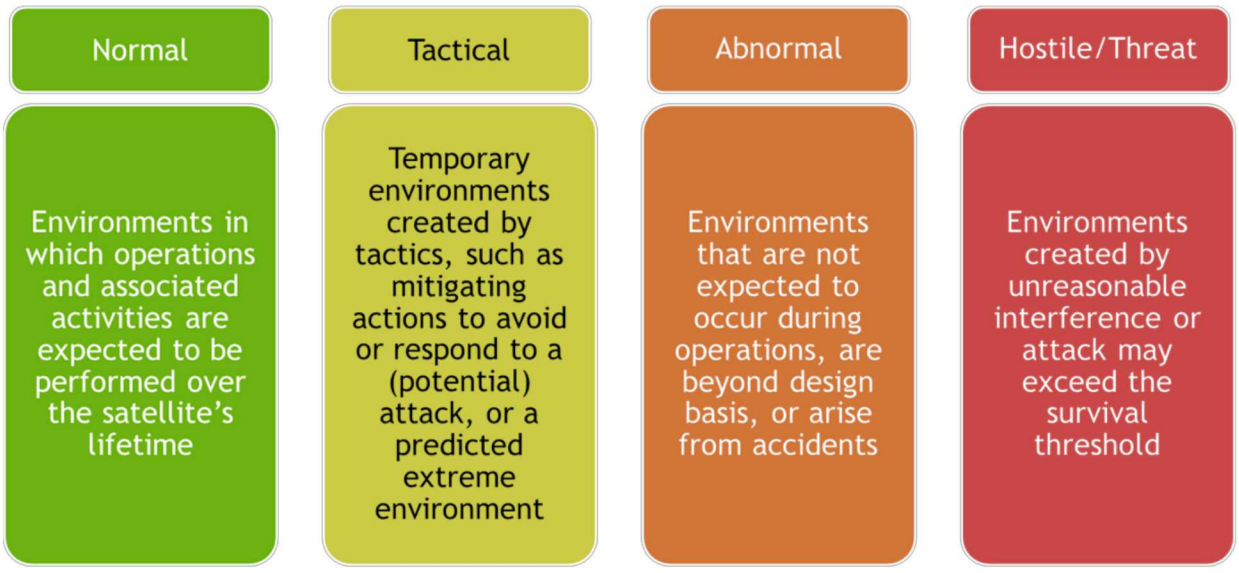

Figure 4-2. Categories of Environments for RPO and OOS

[20] NASA-STD-3000, Volume 1 Man-Systems Integration Standards

Normal and abnormal environments may be naturally occurring or manmade (see Figure 4-3). For example, space weather is naturally occurring, whereas electromagnetic emissions from satellites are often manmade. To put normal and abnormal environments into perspective, a normal operational environment for a satellite over its lifetime might be the 95% level of solar activity—the design basis for operational reliability. A solar environment that exceeds the 95% level is thus a credible environment but may be considered beyond the design basis and is therefore categorized as abnormal. NWs, while not expected to remain operational, must remain safe in credible abnormal environments. A similar requirement might translate to RPO/OOS.

Hostile and tactical environments are by definition manmade. A hostile environment could result from a nuclear detonation releasing radiation into space. Based on design requirements, a satellite may or may not be required to survive hostile radiation environments. Tactical environments result from measures performed by a spacecraft attempting to survive an abnormal environment or malicious (hostile) attack. Examples of a tactical environment might be the change in velocity and orientation to escape, or increased emissions from a counterthreat operation. Note that the uncertainty in knowledge of the environment (or the UUs) is greatest for abnormal and hostile environments and that some environments may be unanticipated or unidentified. Environment uncertainty may also arise from tactical measures.

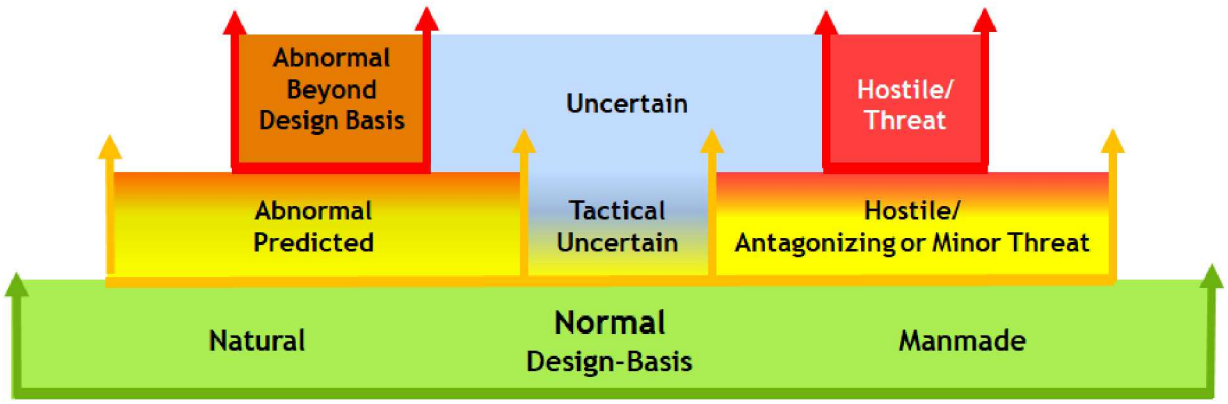

Figure 4-3. Relationship of Environments and Design Basis

4.5.1. Normal Environments

The list of normal RPO/OOS environments includes:

- Orbital maneuvers
- Thermal management
- ESD and charging
- Electromagnetic radiation (EMR) and interference
- Chemical emissions
- Mechanical conditions
- Space weather and radiation
- Electrical settings and operations

4.5.2. Abnormal Environments

Abnormal environments consider credible accidents such as:

- Crash
- Fire, gas or fuel (leak) jetting, or explosion
- Blocked radiators
- Solar power failure
- Contamination from off-gassing or plume impingement
- Unexpected high power EMR
- Extreme naturally occurring conditions—such as solar flare exceeding the 95% worse case solar storm
- Other extreme space weather events

4.5.3. Tactical Environments

Tactical environments include the effects of the following:

- Maneuvering to escape, where orbital parameters are changing
- Generating defensive counterspace actions[21] to impede the Attacker
- Other tactics

4.5.4. Hostile Environments

Hostile environments for RPO/OOSs would be possible threat environments, such as:

- Kinetic energy threats
- Orbital threats; optical backgrounds
- Conducted, radiated e-field and h-field (EMR) interference
- Dispersed high altitude electromagnetic pulse (EMP)
- Atmospheric ionization
- Prompt burst radiation (x-rays, gamma rays, and neutrons)
- Debris decay radiation (short-lived emissions)
- Trapped debris decay betas (electrons)
- Deposited debris

MIL-STD-3053 is an interface standard containing satellite systems in natural and nuclear environments.[22]

4.6. RPO/OOS Scenarios

Development of scenarios aids identification of specific environment types and elucidates reliability and safety needs within the stages and environment categories. Figure 4-4 illustrates three generic scenarios for RPO—cooperative, if between a Servicer and Client; of unknown status, if a Trespasser approaches an orbital Occupant; or aggressive, if an Attacker makes the orbital Occupant

[21] Defense Intelligence Agency, "Challenges to Security in Space" (January 2019)
[22] Department of Defense, Interface Standard, Satellite Systems Natural and Nuclear Environment Standard, MIL-STD-3053, Notice 1, (November 19, 2015); https://www.dsp.dla.mil/Specs-Standards/

a Target. Note that Attackers do not need to be space-based, but for this RPO scenario development they are limited to being space-based.

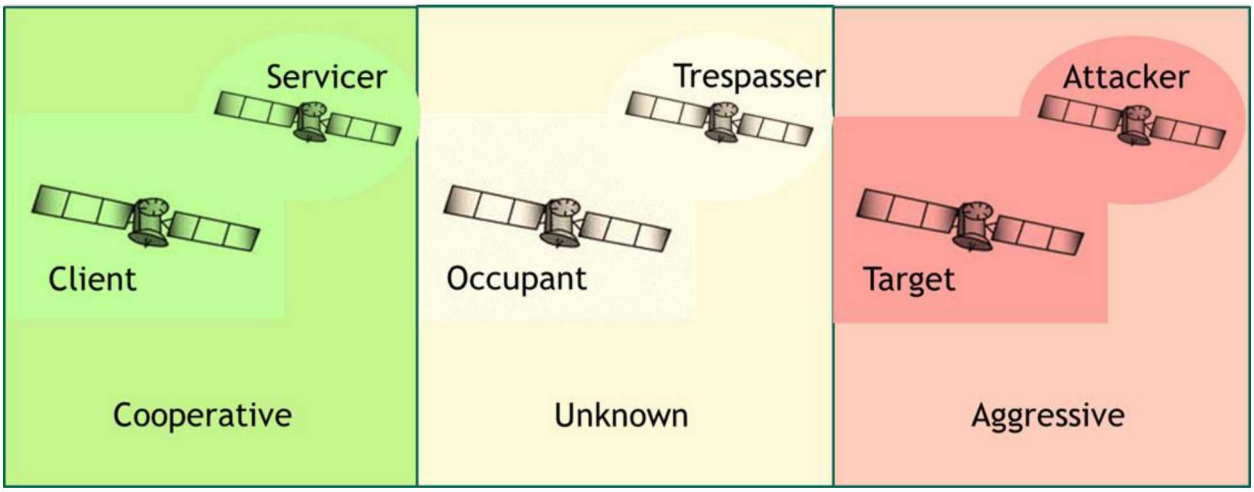

Figure 4-4. Scenarios for RPO/OOS

5. APPYING THE FRAMEWORK TO RPO/OOS SCENARIOS

Next, each scenario will be covered to identify operating modes that adhere to the Always/Never reliability and safety requirements as depicted in Table 2-1. In the following scenarios, it is assumed that the Client and Servicer have communication capabilities and options to undergo mode transitions from normal Operational mode to other modes, such as Service, Safe, Survival, and Recovery. Resulting from discoveries made through scenario analyses, suggestions are made for mode-dependent operations. Authority to proceed with or abort an approach is assumed, but a mechanism for signaling is not suggested. In these scenarios, if only a rendezvous occurs—with no on-orbit servicing—the Dock, Service, and Undock stages would not apply.

5.1. Normal Environment Stages of Servicer-Client Scenario

Using the Always/Never framework, the RPO/OOS operation in normal environments is expected to perform reliably and maintain safety. Table 5-1 shows reliability and safety behaviors for RPO/OOS under normal conditions. The Servicer would transit in Operational mode on a safety collision avoidance (SCA) course towards the Client. On approach, the Client/Servicer communication would indicate authority to proceed; the Client would transition to Service mode, retaining pointing control and removing power except to service components as needed; and the Client and Servicer would transition to Safe mode, adjusting to maximize safety of operations. Safe mode would prevent unsafe conditions and allow State of Health (SOH) checks. The Client and Servicer remain in Service and Safe modes through the dock, service, and undock stages, and then they return to Operational mode and remove Safe mode after departure is completed.

Table 5-1. RPO and OOS Reliability and Safety in Normal Environments

<table>
<tr><th></th><th colspan="2">Client</th><th colspan="2">Servicer</th></tr>
<tr><th>Normal Environment</th><th>Reliability</th><th>Safety</th><th>Reliability</th><th>Safety</th></tr>
<tr><td>Transit</td><td></td><td></td><td>Operational Mode</td><td>Safety collision avoidance (SCA)</td></tr>
<tr><td>Approach</td><td>Signal authority to proceed, change to Service Mode</td><td>Change to Safe Mode</td><td>Given authority to proceed, change to Service Mode</td><td>Change to Safe Mode</td></tr>
<tr><td>Dock</td><td rowspan="3">Service Mode</td><td rowspan="3">Safe Mode</td><td rowspan="3">Service Mode</td><td rowspan="3">Safe Mode</td></tr>
<tr><td>Service</td></tr>
<tr><td>Undock</td></tr>
<tr><td>Depart</td><td>Change to Operational Mode</td><td>Remove Safe Mode</td><td>Change to Operational Mode</td><td>Remove Safe Mode, move to SCA</td></tr>
</table>

5.2. Abnormal Environment Stages of Servicer-Client Scenario

In abnormal environments, the RPO/OOS is not expected to be reliable but should remain safe. If abnormal conditions were detected during transit, the Servicer should withdraw, retaining an SCA course (see Table 5-2).

Note that in reading the table, information applies within a row and not sequentially down a column, because it is assumed the abnormal environment occurs during a stage and not sequentially through the entire RPO/OOS.

If abnormal conditions are encountered during approach, the Client/Servicer communication should abort authority to proceed, the Client and Servicer would transition to Safe mode, and the Servicer would withdraw. If an abort is possible during docking, servicing, or undocking, it might be performed; otherwise, depending for instance on the SOH, the Client would operate critical systems in Service mode and apply Recovery mode as needed. Other systems would operate in Safe mode. The Servicer may have options to attempt service or detach and may need to change from Service mode to Recovery mode depending on the SOH. The Servicer would remain in Safe mode. On departure, SOH would be checked, whereupon Safe modes may be removed and Operational modes resumed.

Table 5-2. RPO and OOS Reliability and Safety in Abnormal Environments

<table>
<tr><th></th><th colspan="2">Client</th><th colspan="2">Servicer</th></tr>
<tr><th>Abnormal Environment</th><th>Reliability</th><th>Safety</th><th>Reliability</th><th>Safety</th></tr>
<tr><td>Transit</td><td></td><td></td><td>Operational Mode</td><td>Withdraw on SCA</td></tr>
<tr><td>Approach</td><td>Abort authority to proceed</td><td>Change to Safe Mode</td><td>Abort</td><td>Withdraw and remain safe and/or change to Safe Mode if needed</td></tr>
<tr><td>Dock</td><td rowspan="3">Abort, or depending on SOH, operate critical systems through in Service Mode and/or apply Recovery Mode as needed</td><td rowspan="3">Operate other systems in Safe Mode</td><td rowspan="3">Depending on SOH, attempt service or detach, otherwise operate critical systems in Service Mode and change to Recovery mode as needed</td><td rowspan="3">Remain in Safe Mode</td></tr>
<tr><td>Service</td></tr>
<tr><td>Undock</td></tr>
<tr><td>Depart</td><td>Check SOH and change to Operational Mode if possible</td><td>Check SOH and remove Safe Mode if appropriate</td><td>Check SOH and change to Operational Mode</td><td>Set SCA and remove Safe Mode if appropriate</td></tr>
</table>

5.3. Hostile Environment Stages of Servicer-Client Scenario

In this scenario, the origin of the hostile environment is not a direct aggressive attack on the servicer or the client. The radiation could instead be merely the collateral effects of a high-altitude nuclear burst that occurs while the RPO/OOS is proceeding. An environment associated with an aggressive attack on the orbital Occupant falls into the next scenario.

Under hostile environment conditions the logic is similar to abnormal conditions above, but the Client and Servicer may be required to operate reliably through the hostile environment. Depending on the nature of the hostile environment and the Client and Servicer requirements, aborting the RPO/OOS may or may not be an allowable option; however, such a requirement was developed for

single spacecraft and not with RPO/OOS in mind. As the nature and needs of RPO/OOS operations can differ from a single spacecraft, reliability during hostile environments is likely mission-dependent.

5.4. Occupant-Trespasser and Target-Attacker Scenarios

When a Trespasser with unknown intentions approaches an orbital Occupant, the environment is uncertain and possibly hostile. The ambiguity may be resolved via a communication from the Trespasser's owner that the approach is unintentional. Tactical avoidance maneuvers may be required of the Occupant, particularly if the Trespasser has limited or no ability to avoid collision.

When a Trespasser approaches and intentions are unconfirmed, the situation may or may not be aggressive. Any form of attack, such that the Occupant becomes a Target, triggers a hostile environment.

In Table 5-3, the Occupant would be synonymous with the Client. However, it is noted that if the RPO/OOS were in progress, the Occupant might refer to both the Client and the Servicer. The Client and the Servicer would try to survive and may individually or together perform tactical countermeasures. The ability of satellites in the docking, servicing, or undocking stages to perform counterspace actions should be considered. The impact of the operations on safety may limit some options. Such scenarios suggest that joint, integrated modes might be considered in the design and development of cooperative Clients and Servicers.

For unknown and aggressive scenarios, the Occupant/Target signals Alert and changes to Survival mode, which—as needed—removes power except to critical components, ceases signals/comms, and/or closes apertures and retracts antennae on instruments. In hostile and tactical situations, uncertainty of environments may exist. At the extreme, a shutdown to deny use, technology, and information may be necessary, followed by a Recovery once the scenario ends and the environments are within normal levels.

Table 5-3. RPO/OOS Tactical and Hostile Attacker Environments

<table>
<tr><th></th><th colspan="2">Occupant</th><th colspan="2">Trespasser/Attacker</th></tr>
<tr><th>Tactical and Hostile Attacker Environments</th><th>Reliability</th><th>Safety</th><th>Reliability</th><th>Safety</th></tr>
<tr><td>Transit</td><td>Signal Alert or receive Alert signal</td><td></td><td rowspan="6" colspan="2">No Control</td></tr>
<tr><td>Approach</td><td>Change to Alert Mode</td><td>Change to Safe Mode</td></tr>
<tr><td>Dock</td><td rowspan="3">Signal Alert and change to Survival Mode</td><td rowspan="3">Survival Mode</td></tr>
<tr><td>Service</td></tr>
<tr><td>Undock</td></tr>
<tr><td>Depart</td><td>Change to Operational Mode using Recovery Mode as Needed</td><td>Remove Safe Modes when appropriate</td></tr>
</table>

This page left blank

6. DISCUSSION

Unmanned RPO/OOS are expected to increase in numbers, but the guidelines for their safety—preventing mission impacts and reducing space debris—are still emerging and may have implications for national security. The Always/Never framework that guides requirements for NW reliability, safety, and security was examined for its possible applicability to unmanned RPO/OOS. The framework and its requirements (Table 2-1) may be overly rigorous for RPO/OOS with only the general requirement of "Do no harm", yet the advantages of adopting and tailoring the framework can still be realized. The following advantages were identified.

The Framework uses Simple Concepts facilitating Ease of Use—

- The "Always/Never" expression and its implications for reliability and safety are easy to remember.
- The safety design principles are encapsulated by the easy to remember principles of Isolation, Incompatibility, Inoperability, Independence, and Elimination. The principles are designed into the system, helping to assure safety in environments.
- The lifecycle stages are limited in number and called by common names.

The Framework allows Derivation of Safety Requirements and Environments for Mission-Specific Situations—The framework applies to the high-level safety objectives and allows derivation of what it means to "remain safe"—making it applicable to many systems and scenarios.

The Framework introduces New Environments, which become More Important as the Space Domain Evolves—The safety basis for space-based operations is largely derived from peaceful (and sometimes manned) missions, whereas the NW safety basis was developed for peacetime and wartime and therefore considers unexpected and hostile conditions. Thus, the NW Always/Never framework brings a fuller set of environments to bear on system design and explains potential causes for unsafety. This consideration is important to both government and commercial spacecraft—conditions that are abnormal or beyond design basis can exist, but hostile environments may need to be considered in light of dual-use missions and aggressive actors. In the event of aggressive acts, satellites may need capabilities to generate Tactical environments.

Safety Requirements in Environments are Consistent—The NW safety basis has well-defined requirements, extensible to RPO/OOS, that allow the effect of an environment on safety design needs to be anticipated. The framework forces remaining safe as the requirement for normal and credible abnormal environments and relies upon understanding the stages of logistics and operations over a system's lifetime.

The Framework can be used as a Shared Guide (or Standard) for RPO/OOS Safety—The adoption and, as appropriate, tailoring of the Always/Never framework standardizes the causes or environments that can impact safety, helps define what is required when in the operational process, and reminds the RPO/OOS community to consider adverse conditions in the space environment sets. By applying the framework to the RPO/OOS scenarios, some standard expectations of behavior arise, calling to attention the possible guidelines for various modes and capabilities within those modes. By adhering to some safety guidelines, potential RPO/OOS for systems not initially intended for coupling may arise—for example, RPO/OOS interactions between government and commercial satellites or one commercial entity's satellite with another commercial entity's satellite.

This page left blank

7. SUMMARY AND CONCLUSIONS

The NW Always/Never safety framework applied to RPO/OOS is useful in that it:

- Drives an unclassified common safety language for the broader community—government and commercial
- Provides rigor consistent with needs for high consequence situations
- Levies standardized requirements on reliability and safety in environments
- Provides a more complete environment set, reminding the community of uncertain and even hostile environments in space
- Presents basic stages and scenarios
- Generates the need for modes of operation

To adopt the NW Always/Never framework, Figure 7-1 indicates the following:

- RPO/OOS safety requirements or guidelines must be developed
- Safety design principles should be articulated
  - A taxonomy around RPO/OOS stages of operation and environments needs to be agreed on to indicate when the requirements/guidelines apply
- Modes of operation should be identified and consistent to communicate expectations between Client and Servicer spacecraft

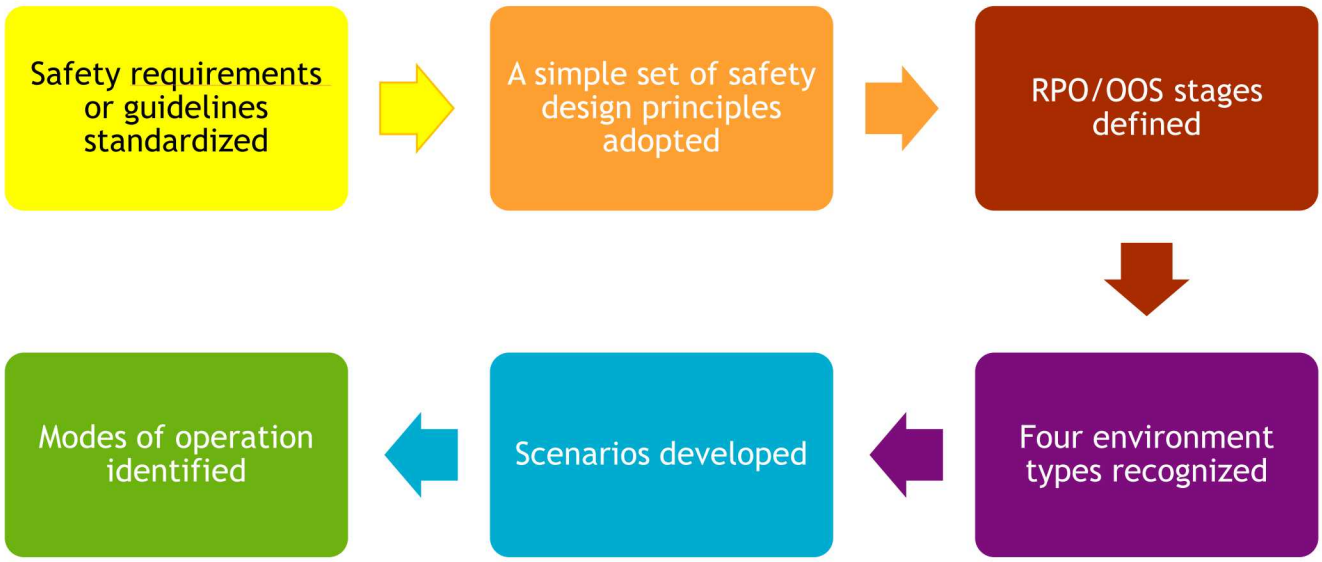

Figure 7-1. Steps in Adopting the Safety Framework

This page left blank

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Mark Ackermann	2830	mracker@sandia.gov;
Tom Nelson	2830	trnelso@sandia.gov;
Neal Brown	2831	nrbrown@sandia.gov;
Steven Trujillo	2832	strujil@sandia.gov;
Celeste Drewien	2833	cadrewi@sandia.gov;
Eva Wallace	2833	etwalla@sandia.gov;
Kim Welch	2834	kmwelch@sandia.gov;
Munaf Aamir	2835	msaamir@sandia.gov;
Kelsey Abel	2835	kabel@sandia.gov;
Sharon Deland	2835	smdelan@sandia.gov;
Nancy Hayden	2835	nkhayde@sandia.gov;
Steve Gianoulakis	6350	segiano@sandia.gov;
Drew Woodbury	6353	dpwoodb@sandia.gov;
Dave Cox	6354	ddcox@sandia.gov;
Jeff Martin	6754	jbmart@sandia.gov;
Roger Byrd	6771	rcbyrd@sandia.gov;
Michele Caldwell	6771	mcaldw@sandia.gov;
Mallory Stewart	6833	malstew@sandia.gov;
Jeff Apolis	8716	jjapoli@sandia.gov;
David Schoenherr	9400	dschoen@sandia.gov;
Scott Slezak	9400	sesleza@sandia.gov;
Technical Library	1977	sanddocs@sandia.gov;

Email—External (UUR)

Name	Company Email Address	Company Name
JJ Hogan	james.j.hogan8.ctr@mail.mil;	SAF/SP
Col. Jason R. Kalainoff	jason.r.kalainoff.mil@mail.mil;	OSD Policy
Maj. Jason T. Brown	jason.t.brown26.mil@mail.mil;	USAF SAF-SP
Audrey Schaffer	audrey.m.schaffer.civ@mail.mil;	OSD Policy
Brian Weeden	bweeden@swfound.org;	Secure World Foundation
Rick Nobbs	rick.nobbs@ati.org;	Advanced Technology International
Frederick Slane	freds@spacestandards.org;	Space Infrastructure Foundation

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.